SECUREPURDUE NEWS
www.purdue.edu/securepurdue

August 2009
Volume 3, Issue 3

All the news that's secure to print.

FROM the CISO

By Scott Ksander
Executive Director
IT Networks & Security

One of the questions I am often asked by vendors who want to get their foot in the door is "What keeps you up at night?" My flip answer is usually "Annoying questions from vendors." A more serious answer would be "What I am going to write about in my next CISO column for SecurePurdue." The honest answer is "What's the next area where we will see security issues?"

If I knew the answer, I would sleep better and, undoubtedly, Purdue would be better prepared. However, my crystal ball doesn't pick up the Future Security Risk Channel. There are a few things, however, that are potential problem areas that we should all keep in mind both as users and service providers.

Web Applications – We have already talked about this some, but this area continues to grow. Just about every application now has a web interface and development and testing practices are all focused on a rush to provide functionality. Few resources are being spent on penetration testing. The AppScan product ITNS is using has helped in the area but we need to keep an eye on developments here and continue to improve our testing technology.

Targeted Phishing – These "spear phishing" attempts continue to get better. The media is also changing from email-based attacks to all forms of social networking. We need to continue our efforts to stop using "hot links" that take our users off to some unknown location. The message is "Don't 'Just Click Here' – ever!"

Partner Connections – As we move more to outsourcing and partnership relationships, we need to understand the risk those data paths create. This is both a technical and relationship problem. There continue to be many unknowns, both benefits and drawbacks, here that we have to explore, but these kinds of connections are inevitable and must be considered carefully.

Unknown Devices – Just about everything these days comes with a network interface and some form of network connection software. Some estimates say that 1.4 billion new network connected devices will ship within the next 2 years. The quality of those connections and available data paths could be a source for great creativity for those searching to exploit insecure paths. I might think twice before connecting my toaster to my home or office network.

The Cloud – Everyone is talking about using "the cloud" for something. However, no one has really defined "the cloud." I don't know about you, but the last time I was flying or driving in a cloud, I didn't feel very secure. Before we "send in the clouds," we need to understand the real values and risk.

As Arseno Hall use to say, "Things that make you go Hmmm ....."
As always, thanks for reading and be careful out there.

In this issue

Internet searches that put you at risk

If you search the web for a song lyric, free music, screen saver or ringtone for your phone, you may be exposing yourself to dangerous content in the sites you visit as well as the items you download. The malware you may come in contact with from these questionable sites and the items you may download from them may compromise your computer and allow malicious individuals and cyber criminals to access personal information such as online banking details.

Searching on the web for popular topics or events increases your risks of compromise. For example, if you checked out the swine flu epidemic, the hackers would have been ready for you. Malicious individuals and cybercriminals are savvy observers of current events that attract large numbers of people. They wait with malware laden sites and files, baiting unsuspecting surfers.

It you search on the web in a popular category, your risks of infection increase.

Searching for popular topics like cool ringtones for your phone or "free music downloads" puts you at risk as well. McAfee has analyzed the risk factor for specific search phrases and found that free music downloads put you at risk 20.7 percent of the time. Screensaver searches put you at the highest risk level with 34.4 percent chance of malware infection.

Our best advice when using your computer on the internet is:

- Do Not open email attachments from unknown sources.
- Before opening an unexpected attachment from a known source verify that the known sender actually sent you the attachment.
- Always keep your anti-virus and anti-malware software and definition files up to date.
- Run anti-spyware programs regularly (daily or weekly).
- Set your operating system to always show file extensions so that you know what kind of file you may be downloading or opening.
- Make sure you keep your browser up to date.
- Stick to trusted web sites; some browser add-ons such as Site Advisor, free from McAfee, will let you know if a site is untrusted.
- Other browser add-ons such as NoScript can be used to disallow execution of scripts on all web pages except the ones you trust and allow.
- Never click on links in emails; always copy and paste them into your browsers address bar.
- Never follow a link in an email that wants you to update account/personal information.
- To see the actual URL link location, hold the mouse pointer over a link (usually displays at the bottom of your browser or as screen tip just beneath the link)
- Always make sure that you are on a secure website before entering personal information; https and the pad lock icon in the bottom of your browser indicates you are on a secure website.

Guidelines for Handling PUID

The data handling guidelines for sending PUID via e-mail have been revised. PUID and NAME may be sent together via e-mail between Purdue business units. Note that PUID is still classified as sensitive University data, and should be handled accordingly.

If you have questions or comments regarding the business use of the PUID, please contact the Identity and Access Management Office at iamo@purdue.edu.

For more information, go to : http://www.purdue.edu/securepurdue/docs/PUIDDataClassif.pdf

SPOTLIGHT

ITNS ePO Service

ITNS offers an anti-malware service via McAfee's ePolicy Orchestrator (better known as ePO). ePO serves as a centralized anti-virus and anti-spyware management solution. Customers access the ePO service through a web-based console which must be run from an authorized workstation. The remote console allows users to run various reports on their ePO managed machines as well as view the tasks and policies assigned to those machines.

ITNS recently upgraded the ePO server from version 3.6.1 to 4.0. Enhancements of version 4.0 include: an improved web-based remote console; Active Directory synchronization; more granular user permissions; expanded reporting capabilities; graphical and customizable dashboards; and much more.

Customers have been given the opportunity to attend training on the updated ePO remote console. The training was conducted by a professional consultant in real-time on the ITNS ePO server.

Today there are approximately 7,700 machines being managed across 35 different departments via the ITNS ePO service. The current list of McAfee products ITNS offers include: VirusScan Enterprise 8.7i, AntiSpyware Enterprise 8.7i, VirusScan 8.6.1 for Mac, and McAfee Agent 4.0 for Windows and Mac. For more information on the ITNS ePO service, including subscription for your department or area, please contact itap-securityhelp@purdue.edu .

October Cybersecurity Events!

Purdue University's Information Technology Networks and Security proudly presents the fourth annual National Cybersecurity Awareness Month during October 2009.
A series of Firewall Chats will be presented in short video vignettes beginning in October and continuing through the rest of 2009.

This year's events will focus on computer security topics with our traditional Halloween security costume contest.

WHEN: **October 30, from 9 to 11 a.m.**
WHERE: **Fowler Hall in Stewart Center**

John McCumber, will be presenting on the industry threats. He is a strategic programs manager in the Public Sector Group of Symantec Corp. Scott Ksander, CISO of IT Networks and Security will present on University threats. Our traditional Halloween Security costume contest will conclude this session.
Check http://www.purdue.edu/securepurdue/training for event updates.

SECURITY RESOURCES

Use the following resources to educate yourself about security and privacy issues surrounding computers and data networks.

- *Purdue University IT Resource Acceptable Use Policy*

http://www.purdue.edu/policies/pages/information_technology/v_4_1.html

- *SecurePurdue Website*

http://www.purdue.edu/securepurdue/training
http://www.purdue.edu/securepurdue/docs/PUIDDataClassif.pdf

Trustees approve vendor for campus network upgrade, software agreement

WEST LAFAYETTE, Ind. — Purdue's board of trustees on Friday (July 10) approved an Indianapolis-based vendor for the university's new information technology infrastructure initiative and a Microsoft software agreement.

Verizon Business Network Services from Indianapolis is the vendor that will handle Purdue's five-year, $24 million network infrastructure project, Purdue Network 2010. The project will update Purdue's network and establish a strategic partnership with a future vendor to sustain the infrastructure over a multiyear period.

"This initiative will modernize and build a reliable infrastructure to support mobile communication, such as voice, video and data, for Purdue's research, teaching, learning and business needs," said James S. Almond, vice-president for business services and assistant treasurer. "Upgrading our data network is a must for Purdue to achieve the goals in Purdue's strategic plan.

"Our network has served us well since it was installed in the mid-1990s as one of the first modern computing and telecommunications networks at a university. However, the network is showing its age both in terms of wornout equipment and outdated capabilities. Increased demands created by video use, wireless smart phones and the relentless appetite for data in research are clogging the Purdue network."

Part of the project's focus will be securing equipment to address functions related to wireless services, services between campus buildings and connectivity within academic buildings.

The West Lafayette campus network infrastructure currently provides wired communications services to more than 61,000 locations on campus. The wireless network covers 3.7 million interior square feet in 255 campus buildings thanks to more than 1,800 access points.

However, today's campus network is not redundant, and a single failure has the potential to remove service to hundreds of campus users, said Gerry McCartney, the Olga Oesterle England Professor of Information Technology and vice president for information technology and chief information officer. More than half of the network's 3,000 devices, such as switches and routers, have reached the end of their lifecycles and have no upgrades. There also are significant gaps in the wireless coverage.

"Purdue Network 2010 will strengthen the West Lafayette campus infrastructure and allow Purdue to meet current demand for networking resources and accommodate future demand," McCartney said. "Our goals include providing superior wireless connectivity to campus users, as well as improving campus desktop support, increasing security and providing incentive for companies to relocate or launch in Purdue Research Park.

"The strategic learning, research and collaborative opportunities for advancement with a robust, reliable network infrastructure are endless."

In other business, the trustees also approved a $3.4 million contract with Software House International of Piscataway, N. J., to renew the Microsoft Campus and School Agreement, which allows Purdue to license a variety of Microsoft software for faculty, staff and student use at a substantial discount. The license fee for each faculty and staff member is $41.70 for all three years of the term and an average of $13.08 per student annually. Over three years, the contract is projected to save Purdue $239,130.

Writer: Amy Patterson Neubert, 765-494-9723, apatterson@purdue.edu
Source: James S. Almond, 765-494-9706, jsalmond@purdue.edu
Gerry McCartney, 765-496-2270, mccart@purdue.edu
Related Web sites:
Information Technology at Purdue: http://www.itap.purdue.edu/